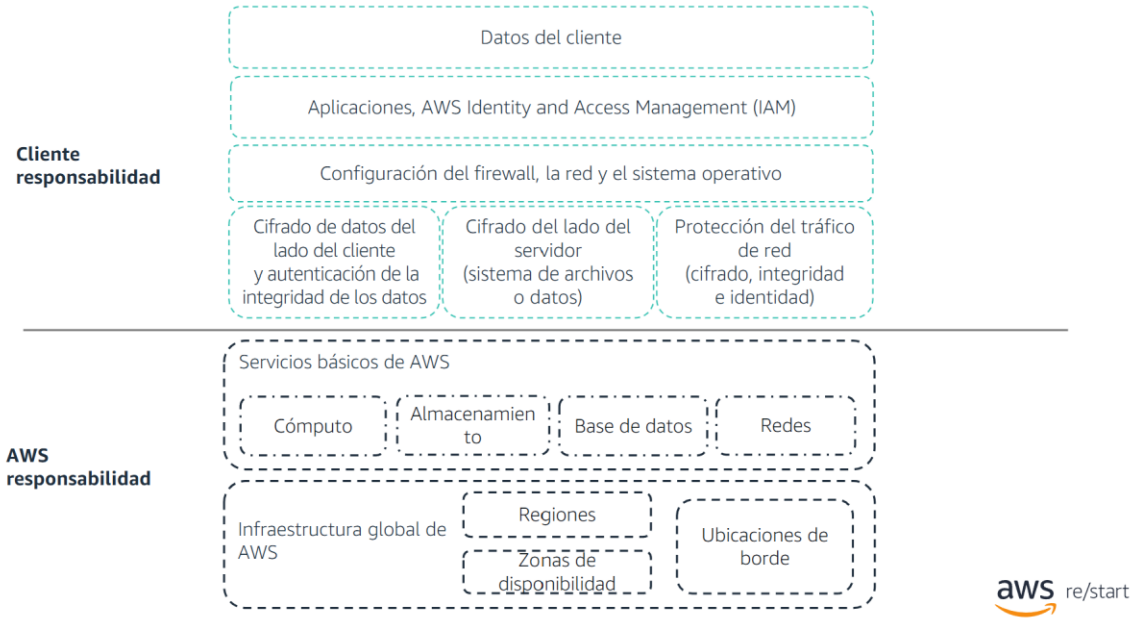
Modelo de responsabilidad compartida de AWS

Modelo de responsabilidad compartida

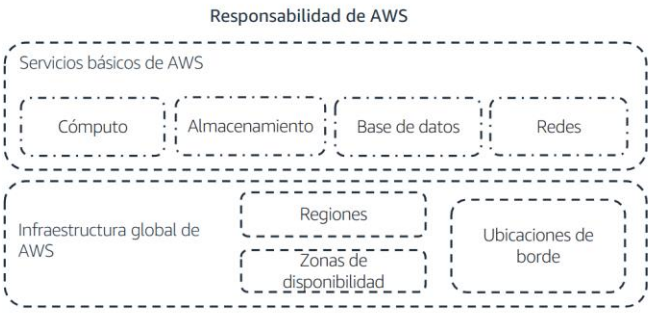


aws re/start

Responsabilidades de seguridad de AWS: Seguridad **DE** la nube

Seguridad de la nube

- Seguridad física de los centros de datos:
  - Acceso controlado y basado en las necesidades
- Infraestructura de hardware y software:
  - Retirada del almacenamiento, auditoría y registro de acceso al sistema operativo (SO) del anfitrión
- Infraestructura de red:
  - Detección de intrusos
- Infraestructura de virtualización:
  - Aislamiento de instancias



Responsabilidades de seguridad de los clientes: Seguridad **EN** la nube

Seguridad en la nube

- SO de Instancia de Amazon Elastic Compute Cloud (Amazon EC2)
  - Incluidos parches y mantenimiento
- Aplicaciones
  - Contraseñas, acceso basado en roles y otros
- Configuración del grupo de seguridad
- Firewalls basados en el sistema operativo o en anfitrión
  - Incluidos sistemas de detección o prevención de intrusos
- Configuraciones de red
- Administración de cuentas
  - Configuración de inicio de sesión y permisos para cada usuario

aws re/start

Características del servicio y responsabilidad de seguridad

Infraestructura como servicio (IaaS)

- El cliente tiene más flexibilidad en cuanto a la configuración de las opciones de red y almacenamiento
- El cliente es responsable de administrar más aspectos de la seguridad
- El cliente configura los controles de acceso

Plataforma como servicio (PaaS)

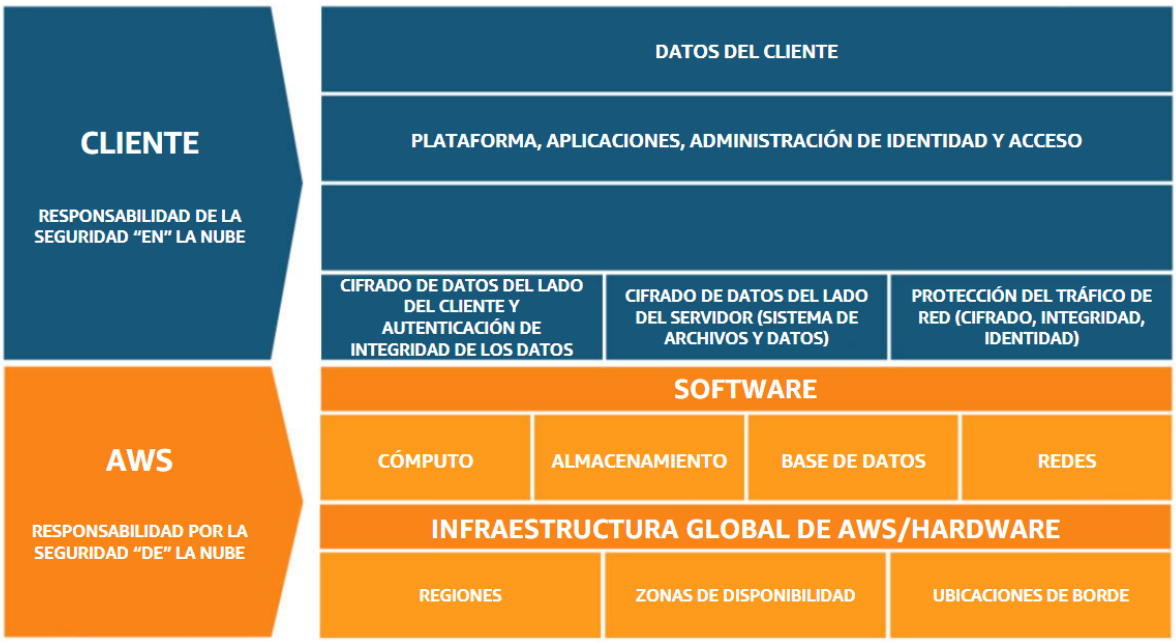
- El cliente no necesita administrar la infraestructura subyacente
- AWS gestiona el sistema operativo, la aplicación de parches de bases de datos, la configuración del firewall y la recuperación de desastres (DR)
- El cliente puede centrarse en administrar código o datos

aws re/start

Características del servicio y responsabilidad de seguridad (continuación)

Software como servicio (SaaS)

- El software se encuentra alojado de forma centralizada.
- Licencia basada en un modelo de suscripción o de pago por uso.
- Por lo general, se accede a los servicios a través de un navegador web, una aplicación móvil o una interfaz de programa de aplicación (API).
- Los clientes no necesitan administrar la infraestructura que soporta el servicio.



Preguntas y respuestas

Considere esta implementación. ¿Quién es el responsable: AWS o el cliente?

1. ¿Actualizaciones y parches del sistema operativo en la instancia EC2?
   - RESPUESTA: El cliente
2. ¿Seguridad física de los centros de datos?
   - RESPUESTA: AWS
3. ¿Infraestructura de virtualización?
   - RESPUESTA: AWS
4. ¿Configuración del grupo de seguridad de Amazon EC2?
   - RESPUESTA: El cliente
5. ¿Configuración de las aplicaciones que se ejecutan en la instancia EC2?
   - RESPUESTA: El cliente
6. Actualizaciones o parches de Oracle, si la instancia de Oracle se ejecuta como instancia de Amazon RDS?
   - RESPUESTA: AWS
7. ¿Actualizaciones o parches de Oracle si Oracle se ejecuta en una instancia EC2?
   - RESPUESTA: El cliente
8. ¿Configuración del acceso al bucket de S3?
   - RESPUESTA: El cliente

Aprendizajes clave

- AWS y el cliente comparten las responsabilidades en torno a la seguridad
  - AWS es responsable de la seguridad **de** la nube
  - El cliente es responsable de la seguridad **en** la nube
- **AWS es responsable de proteger la infraestructura** (incluidos el hardware, el software, las redes y las instalaciones) que ejecutan los servicios en la nube de AWS.
- En el caso de los servicios que se clasifican como infraestructura como servicio (IaaS), el **cliente es responsable de realizar las tareas de configuración y administración de seguridad necesarias**
  - Por ejemplo, actualizaciones del SO invitado y parches de seguridad, firewall, configuraciones de grupos de seguridad.